INTERNAL INSPECTIONS REPORT

IT OPERATIONS

Prepared By:
[Insert Agency]
[Insert Agency Address]

[Insert Data Center Location]
[Insert Data Center Address]

[Insert Date]

INSTRUCTIONS

The following questions serve as an internal audit checklist regarding the agencies security procedures relating to Internal Revenue Service documents and federal security implementation controls. The purpose of this questionnaire is to measure the agencies level of compliance with federal disclosure regulations.

When answering the questions in this document, the answers should be entered on the line directly below the question. Formatting and color for the answer has already been set, so modifying this it not advisable. The responses will be colored blue, so it's easily identifiable. For Example:

1. How is FTI received from the IRS?

   FTI is received from the IRS via the secure Tumbleweed client to a Windows XP workstaion.

After completion, the form should be printed out and signed by the Disclosure Officer and the Director from the Agency.

The Agency should complete the contact information below for all parties that involved in supplying information.

Name	Title	E-mail

It is advisable for the agency to collect and maintain documented evidence to back to answers to this report in the instance of an audit. Having this evidence on hand will also aid the IRS Safeguards on-site review.

Record Keeping Requirements (Publication 1075 section 3.0) IRC Section 6103(p)(4)(A)

1. How is FTI received from the IRS? (Tumbleweed, ConnectDirect, other Secure Data Transmission (SDT)-list)

2. Are FTI receipts logged ?

    a. What data elements are captured in the log?

3. Upon receipt of FTI, how and where is the data electronically distributed?

4. What electronic media do you still have and how are you planning disposal?

5. Is electronic media provided to a contracted State Agency or Contractor?

    a. List

    b. What safeguard controls are in place when transmitting and processing the electronic media at this site?

6. Where is electronic media stored before and after processing? (Agency, Data Center, Other-list)

    a. Is electronic media with FTI stored with other Agency data?

7. How are data files backed up, by whom, and on what type of media? Please include information regarding all data back-ups, including local servers, allowed contractors and dispersement units.

8. What is the retention period of back-up media and how many generations of back-up files exist at this time?

9. Are back-up files stored off-site?

    a. Where (Site Name and address) are files stored?

    b. What protections are in place?

    c. Who currently has access (name & title)?

Secure Storage (Publication 1075 section 4.0) IRC Section 6103(p)(4)(B)

10. Please describe the physical security of the Data Center? (e.g. keypad locked doors, guard desks, locations, hours, etc.)

    a. If keypads are used, is each attempt logged?

    b. Who reviews the access attempt logs? (Name and title)

11. What alarm systems are currently running at Data Center? (e.g. Intrusion Alarms, Motion Detectors, Exit Alarms)

    a. Who monitors these alarms? (Name and title)

12. Are security cameras used at the Data Center?

    a. Who monitors the security feed? (Name and title)

13. Are records maintained on the issuance of keys/key cards?

a. How are records maintained? (automated file, written log, etc.)

b. Who is responsible for the issuance of keys/key cards (Name and title)

c. Are periodic reviews conducted to reconcile records and determine if users still need access?

  i. Date of last review.

14. Is FTI locked in a storage cabinet?

a. Where is the key kept?

b. Who has access to the key?

c. How many keys are in existence?

d. Who maintains the backup keys?

15. Are combination locks used?

a. How often is the combination changed?

b. Who controls the combinations?

16. Are ID cards required to be worn by employees at all times?

a. How are ID cards inventoried or managed?

17. Do visitors/vendors sign a visitor access log?

  a. What data elements are captured in the log?

  b. Who reviews the visitor access log periodically?

18. Two barriers are required to protect FTI. Please Describe the one that applies to your agency:
  i. Secured perimeter / locked container
  ii. Locked perimeter / secured interior
  iii. Locked perimeter / secured container
  iv. Other (describe)

19. Who has access to the Data Center after core business hours?

  a. How is security enforced after core business hours?

20. Is this a state-run facility or a contractor site?

  a. How access limited from non-agency personnel?

Restricting Access (Publication 1075 section 5.0) IRC Section 6103(p)(4(C)

21. What identifying information is used to retrieve FTI?

22. Is FTI kept separate or is it commingled with other information?

23. Can FTI within agency records be located and separated easily?

24. How is access limited to authorized personnel?

25. Is FTI made available to personnel outside of agency personnel (contractors, other agencies, etc.)?

   a. List personnel/offices and provide a justification.

26. Are FTI access log reports monitored to detect unauthorized browsing?

Disposing Federal Taxpayer Information (Publication 1075 section 8.0) IRC Section 6103(p)(4)(F)

27. Is FTI stored on electronic media (tapes)?

   a. How is the data erased? (Degaussed, Written over with 0 (zero) and 1 (one), Written over with new data)

Computer System Security (Publication 1075 section 5.6)

28. How are accounts managed for network access?

   a. Who manages the accounts?

   b. Are accounts given the appropriate level of permissions that do not exceed a persons need for their job functions?

   c. How often and by whom are accounts reviewed for access need?

d. Are accounts configured to lock after 3 failed login attempts?

29. Are users supplied with unique user IDs?

a. How does the user receive their network user ID?

b. Are user IDs disabled after 90 days of inactivity?

c. Are user IDs archived?

30. Are network passwords set to be a minimum of 8 characters in length?

a. What complexity requirements are tied to passwords?

b. Are passwords required to be changed at least every 90 days?

c. How many generations of passwords are maintained?

31. Is an IRS approved warning banner displayed prior to a user login?

32. Are workstations required to go to a screen saver / hibernate mode after 15 minutes of inactivity?

a. Are users required to enter a password when recovering from a screen saver / hibernate mode?

33. Are servers that store, transmit, or process FTI configured to terminate sessions after 15 minutes of inactivity?

34. Is auditing enabled on the application?

a. What software is used to manage auditing on the network?

b. What auditable events are set to be captured?

c. Is appropriate storage capacity given to audit records?

d. Are there alerts established to inform administrators of an audit processing failure?

i. How is the administrator alerted?

e. Does the software used to manage auditing provide capabilities for monitoring, analyzing, and report generation of auditable events?

i. Does the reporting feature allow for reduction, so that reports on specific audit events can be tailored to a report?

f. Are time stamps used with each audit event?

g. How is the audit information protected?

h. How long are audit records maintained?

35. Does the Agency provide annual security awareness training?

a. Are there records maintained to track employee completion of this training?

36. Does the Agency provide job-related security training?

a. Are there records maintained to track employee completion of this training?

37. Does the Agency utilized the Plan of Actions and Milestones (POA&M) process to manage risks identified through security assessments or risk assessments?

38. Is a baseline configuration maintained for the application that contains software versions, patch levels, services used, etc.?

a. Are deviations from the baseline configuration documented?

39. Does the Agency follow a configuration change control process?

a. How are change requests submitted?

b. Who analyzes the requests?

c. Is there an established Configuration Control Board that is involved in the approval process?

d. Are all changes to the information system documented?

40. Is there a list of personnel who are authorized to make changes to the application?

a. Is this list of personnel periodically reviewed?

41. Is a list of prohibited/restricted functions, ports, protocols, and services identified and maintained?

42. Is a component inventory maintained to track all network assets?

a. What elements are captured in the inventory? (e.g. manufacturer, model number, serial number, software license information, owner, etc.)

43. Is there a disaster recovery site or alternate processing facility?

a. Are failover tests conducted and how often?

i. What is the date of the last test?

44. What software and version is used for Virus Protection?

45. What software and version is used for Intrusion Detection?

46. What software and version is used for Spam/Spyware Protection?

47. Does network traffic, with regards to systems that FTI bypasses, utilize encryption?

   a. Explain the type of encryption used.

48. What tools, to include their purpose, are used to perform network and system maintenance?

49. Is remote maintenance performed?

   a. How are the remote maintenance sessions protected?

50. Is a list of personnel authorized to perform maintenance maintained?

51. Is there an established Rules of Behavior that describes user responsibilities and expected behavior?

   a. Are users required to read and sign a statement (that’s kept on file) indicating acknowledgement?

52. Are vulnerability scans conducted on the network?

   a. What software is used for vulnerability scanning?

   b. How often are vulnerability scans conducted?

   c. Are the results of the vulnerability scans maintained?

   d. When was the last vulnerability scan conducted?

53. Is there a list of software that is prohibited from used maintained?

54. Are there usage restrictions on mobile code (Java, JavaScript, ActiveX, Postscript, Shockwave, Flash, and VBscript)?

I hereby submit this Internal Inspections Report to the headquarters function of this agency as part of the IRS Safeguards Internal Inspections requirement.

/s/

____ _____________

Field Office Official Conducting Internal Inspection Date

I acknowledge that I reviewed this Internal Inspections Report as part of the IRS Safeguards Internal Inspections requirement and initiated appropriate corrective actions for any deficiencies identified.

/s/

____ _____________

Agency Disclosure Officer Date

/s/

____ _____________

Agency Official Date